PRIMUS PARTNERS®
Solutions for Tomorrow

Quote by Arun Moral, Managing Director, Primus Partners

Published in TechCircle
November 18, 2025

Data Centre firms brace for stronger controls and higher costs under DPDP Rules 2025

Read on: Data Centre firms brace for stronger controls and higher costs under DPDP Rules 2025

Article Content:

The Ministry of Electronics and Information Technology notified the Digital Personal Data Protection (DPDP) Rules 2025 last Friday for the full operationalisation of the DPDP Act 2023. It lays out a staggered mechanism for implementing data protection mandates over a period of up to 18 months.

It also set in motion a profound transformation across the country's data infrastructure, particularly within data centres. While data centers are typically in the role of processors (they host and process data on behalf of clients), the DPDP Rules assign them a much more central role in compliance.

Under the new rules, data fiduciaries (i.e., companies that collect and control data) are mandated to implement 'reasonable security safeguards', a requirement that extends to their processors — meaning data centres.

The most immediate change comes from the heightened security expectations built into the DPDP regime. The law places the compliance burden on data fiduciaries to ensure that their processors, including data centres, follow the same standards. By extension, data centres will have to strengthen their internal systems, improve access controls, adopt stronger encryption, and maintain continuous logs of data activity. The rules also require prompt reporting of data breaches, which effectively places data centres in the frontlines of incident detection and response. If a customer suffers a breach, the data centre's ability to identify the incident and provide forensic information will become a regulatory necessity rather than a service add-on.

"For customers for whom we are a co-location provider, wherein customers' hardware is hosted with us, we have no access to any applications or data, and DPDP does not apply. In cases where we provide cloud services (Infrastructure as a service & Platform as a service), there are implications to us," said A.S. Rajgopal, MD & CEO of NxtGen Cloud Technologies, a data centre and cloud services provider.

He explained that they plan to encrypt their entire storage so that no one can access the data in the event of a breach at their end. Rajgpal added that they would also encrypt customer buckets using encryption keys owned by the customers themselves, along with deploying stronger access controls. Customers are also exploring technologies such as masking and tokenisation to protect the personal data of their own end users.

NxtGen already maintains detailed audit logs and, although their current retention period was six months, they intend to increase it to one year. He added that they now had a Data Protection Officer in addition to a CISO.

RackBank has revised all Data Processing Agreements, Master Service Agreements, and Service Level Agreements to ensure perfect alignment with the statutory role of a Data Processor under the DPDPA, said Narendra Sen, Founder & CEO. These Agreements include detailed clauses on data retention, deletion assistance, access management, and sub-processor disclosures.

“Our infrastructure is being engineered to exceed DPDP expectations so that every enterprise, financial institution, and government partner can innovate with the assurance that their data and their compliance obligations are fully protected,” he added.

The DPDP Rules 2025 have set clear expectations for data-centre security by mandating encryption or masking of personal data, controlled system access, monitored logging with one-year retention, and verified data backups to ensure continuity of processing.

“These requirements transform security from a periodic checklist into or real-time checklist and operational responsibility. While some operators already have structured logging, access controls, and backup processes, others will need to strengthen these measures and invest in advanced capabilities like SOC, SIEM, DDoS protection, and immutable backups,” said Sundareshwar Krishnamurthy, Partner and India Cyber Leader at PwC India.

Increase in CapEx and OpEx

Experts opine that DPDP-driven infrastructure upgrades would require new hardware, software, and architectural changes, including secure storage for sensitive personal data, data-flow mapping layers and classification engines, dedicated systems for audits, analytics, and consent management, and enhanced logging, encryption, and key-management modules. These additions are expected to directly raise upfront acquisition, integration, and installation costs.

Further, data-localisation requirements under the DPDP rules would compel multinational firms to build or lease onshore facilities, migrate workloads away from offshore clouds, and create parallel India-only clusters and containers.

Construction expenses have already been rising at 5–10% annually, driven by higher input prices, supply-chain pressures, and growing demand for in-country processing. As a result, building new capacity has become significantly more expensive, with each additional 1 MW of data-centre power now costing between USD 4–5 million (₹35–45 crore), said Arun Moral – Managing Director at consulting firm Primus Partners.

The operational burden is increasing just as quickly. Organizations now need to fund expanded compliance and governance functions, including the appointment of Data Protection Officers, ongoing risk assessments, consent-lifecycle management, personal-data mapping, erasure workflows, and continuous audit trails. This translates into higher recurring spends on technology, skilled manpower, training, and monitoring systems.

As per Ernst and Young’s estimates, DPDP will create a significant compliance ecosystem in India, with an estimated upwards of ₹10,000 crore opportunity over the next three years across privacy automation and compliance services. It will be similar, albeit smaller in scale, to the European privacy mandate GDPR that required 27 EU countries to overhaul their systems simultaneously.

Finally, the financial risk of non-compliance has become a major cost driver by itself. With penalties that can go up to ₹250 crore for severe violations or breaches, organizations are increasingly compelled to invest in preventive controls, cyber-insurance coverage, and automated compliance frameworks to mitigate exposure.